FortiOS™ Handbook - Life of a Packet

VERSION 5.2.4

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

November 10, 2015

FortiOS™ Handbook - Life of a Packet

TABLE OF CONTENTS

Change Log

Date	Change Description
November 10, 2015	Corrections to the High-level packet flow diagram in Packet flow on page 6.
October 18, 2015	Initial publication.

Introduction

Directed by security policies, a FortiGate unit screens network traffic from the IP layer up through the application layer of the TCP/IP stack. This chapter provides a general, high-level description of what happens to a packet as it travels through a FortiGate unit running FortiOS 5.2.x.

The FortiGate unit performs three types of security inspection:

- Stateful inspection, that provides individual packet-based security within a basic session state
- Flow-based inspection, that takes a snapshot of content packets and uses pattern matching to identify security threats in the content
- Proxy-based inspection, that reconstructs content passing through the FortiGate unit and inspects the content for security threats.

Each inspection component plays a role in the processing of a packet as it traverses the FortiGate unit en route to its destination.

How this guide is organized

This FortiOS Handbook chapter contains the following sections:

Packet flow describes the life of a packet as it passes through a FortiGate unit

Comparison of inspection types shows how different security functions map to different inspection types.

Client/Server connection packet flow example

Routing table update packet flow example

Dialup IPsec VPN with Application control example

Packet flow

After the FortiGate unit's external interface receives a packet, the packet proceeds through a number of steps on its way to the internal interface, traversing each of the inspection types, depending on the security policy and security profile configuration. The diagram below is a high level view of the packet's journey.

The description following is a high-level description of these steps as a packet enters the FortiGate unit towards its destination on the internal network. Similar steps occur for outbound traffic.

Packet flow consists of the following modules:

Ingress packet flow

- Interface TCP/IP stack
- DoS Sensor
- IP integrity header checking
- IPsec VPN
- Destination NAT (DNAT)
- Routing

Stateful inspection

- Local Management Traffic
- Policy Lookup
- Session Tracking
- Session helpers
- SSL VPN
- User Authentication
- Traffic Shaping

Flow-based inspection

- IPS
- Application Control
- Web Filter
- DLP
- Antivirus

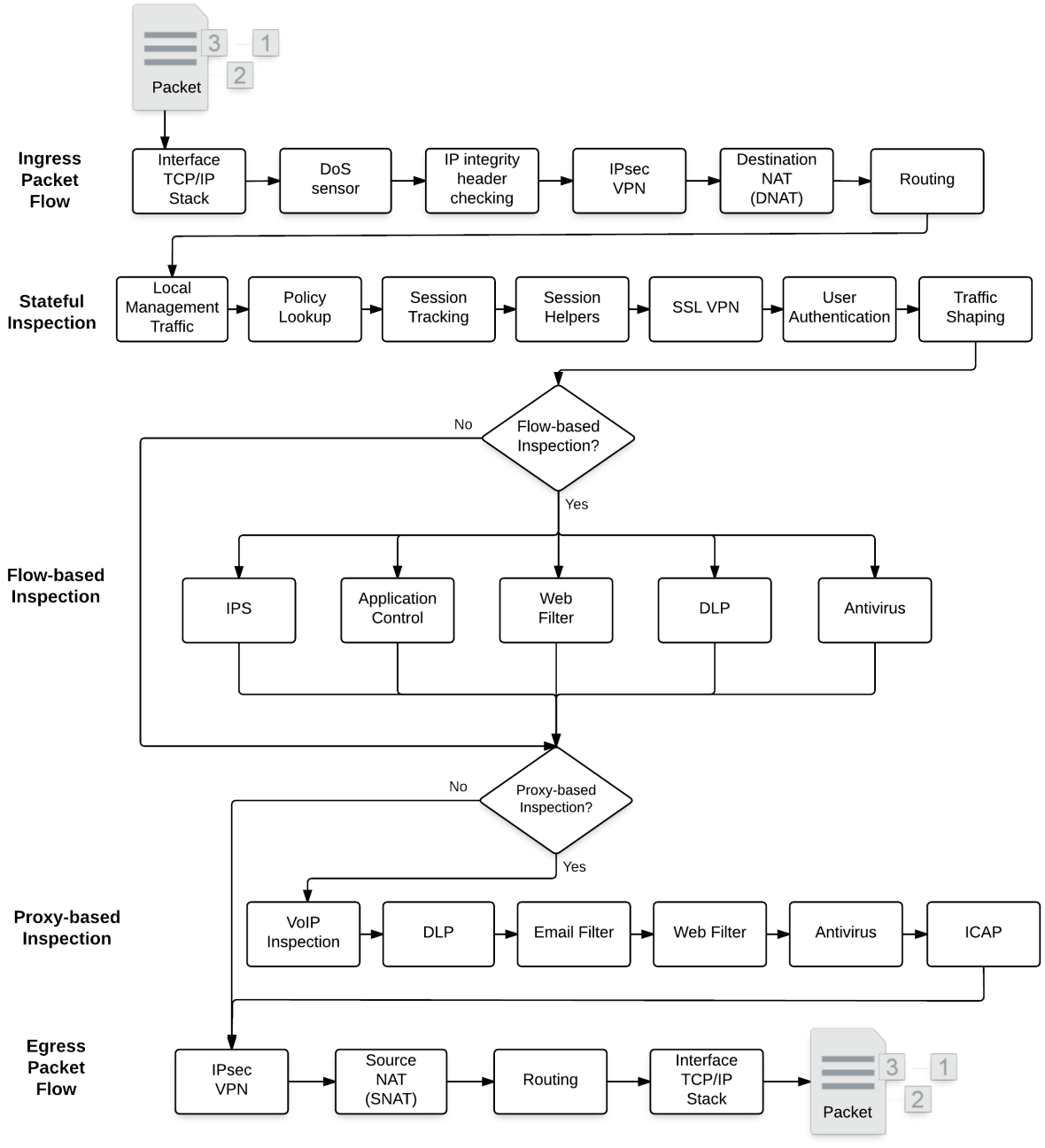
Proxy-based inspection

- VoIP Inspection
- DLP
- Email Filter
- Web Filter
- Antivirus
- ICAP

Egress packet flow

- IPsec VPN
- Source NAT (SNAT)
- Routing
- Interface TCP/IP stack

High-level Packet flow diagram



Ingress packet flow

When a packet is received by an interface and enters a FortiGate the following steps occur:

Interface TCP/IP stack

Ingress packets are received by a FortiGate interface.The packet enters the system, and the interface network device driver passes the packet to the Denial of Service (DoS) sensors, if enabled, to determine whether this is a valid information request or not.

DoS sensor

DoS scans are handled very early in the life of the packet to determine whether the traffic is valid or is part of a DoS attack.The DoS module inspects all traffic flows but only tracks packets that can be used for DoS attacks (for example, TCP SYN packets), to ensure they are within the permitted parameters. Suspected DoS attacks are blocked, other packets are allowed.

IP integrity header checking

The FortiGate unit reads the packet headers to verify if the packet is a valid TCP, UDP, ICMP, SCTP or GRE packet. The only verification that is done at this step to ensure that the protocol header is the correct length. If it is, the packet is allowed to carry on to the next step. If not, the packet is dropped.

IPsec VPN

If the packet is an IPsec packet, the IPsec engine attempts to decrypt it. If the IPsec engine can apply the correct encryption keys and decrypt the packet, the unencrypted packet is sent to the next step. Non-IPsec traffic and IPsec traffic that cannot be decrypted passes on to the next step without being affected.

Destination NAT (DNAT)

The FortiGate unit checks the NAT table and determines if the destination IP address for incoming traffic must be changed using DNAT. DNAT is typically applied to traffic from the Internet that is going to be directed to a server on a network behind the FortiGate. DNAT means the actual address of the internal network is hidden from the Internet. This step determines whether a route to the destination address actually exists.

DNAT must take place before routing so that the FortiGate unit can route packets to the correct destination.

Routing

The routing step uses the routing table to determine the interface to be used by the packet as it leaves the FortiGate unit. Routing also distinguishes between local traffic and forwarded traffic. Firewall policies are matched with packets depending on the source and destination interface used by the packet. The source interface is known when the packet is received and the destination interface is determined by routing.

Stateful inspection

Stateful inspection looks at the first packet of a session and looks in the policy table to make a security decision about the entire session. Stateful inspection looks at packet TCP SYN and FIN flags to identity the start and end of a session, the source/destination IP, source/destination port and protocol. Other checks are also performed on

the packet payload and sequence numbers to verify it as a valid session and that the data is not corrupted or poorly formed.

When the first packet is a session is matched in the policy table, stateful inspection adds information about the session to its session table. So when subsequent packets are received for the same session, stateful inspection can determine how to handle them by looking them up in the session table (which is more efficient than looking them up in the policy table).

Stateful inspection makes the decision to drop or allow a session and apply security features to it based on what is found in the first packet of the session. Then all subsequent packets in the same session are processed in the same way.

When the final packet in the session is processed, the session is removed from the session table. Stateful inspection also has a session idle timeout that removes sessions from the session table that have been idle for the length of the timeout.

See the Stateful Firewall Wikipedia article (https://en.wikipedia.org/wiki/Stateful_firewall) for an excellent descruption of stateful inspection.

Local management traffic

Local management traffic terminates at a FortiGate interface. This can be any FortiGate interface included dedicated management interfaces. In multiuple VDOM mode local management traffic terminates at the management interface. In Transparent mode, local management traffic terminates at the management IP address.

Local management traffic includes administrative access, some routing protocol communication, central management from FortiManager, communication with the FortiGuard network and so on. Management traffic is allowed or blocked according to the Local In Policy list which lists all management protocols and their access control settings. You configure local management access indirectly by configuring administrative access and so on.

Management traffic is processed by applications such as the web server which displays the FortiOS web-based manager, the SSH server for the CLI or the FortiGuard server to handle local FortiGuard database updates or FortiGuard Web Filtering URL lookups.

Local management traffic is not involved in subsequent stateful inspection steps.

SSL VPN traffic terminates at a FortiGate interface similar to local management traffic. However, SSL VPN traffic uses a different destination port number that administrative traffic and can thus be detected and handled differently.

Policy lookup

The first stateful inspection step is a policy lookup that matches the packet with a firewall policy based on standard firewall matching criteria (source and destination interfaces, source and destination IP addresses, and port numbers). If the policy denies the packet it is discarded. An accepted packet continues to the next step.

Many FortiOS features are applied to traffic depending on the settings in the policy that matches the traffic as determined by the policy lookup. This includes authentication, security features and so on.

Session tracking

As described above for stateful inspection. Sessions are tracked in a session table after policy lookup has identified a new session.

Session helpers

Some protocols include information in the packet body (or payload) that must be analyzed to successfully process sessions for this protocol. For example, the SIP VoIP protocol uses TCP control packets with a standard destination port to set up SIP calls. To successfully process SIP VoIP calls, FortiOS must be able to extract information from the body of the SIP packet and use this information to allow the voice-carrying packets through the firewall.

FortiOS uses session helpers to analyze the data in the packet bodies of some protocols and adjust the firewall to allow those protocols to send packets through the firewall. FortiOS includes the following session helpers:

- PPTP
- H323
- RAS
- TNS
- TFTP
- RTSP
- FTP
- MMS
- PMAP
- SIP
- DNS-UDP
- RSH
- DCERPC
- MGCP

SSL VPN

Local SSL VPN traffic is treated like special management traffic as determined by the SSL VPN destination port. Packets are decrypted and are routed to an SSL VPN interface. Polcy lookup is then used to control how packets are forwarded to their destination outside the FortiGate.

User Authentication

User authentication added to security policies is handled by the stateful inspection, which is why Firewall authentication is based on IP address. Authentication takes place after policy lookup selects a policy that includes authentication.

Traffic Shaping

If the policy that matches the packet includes traffic shaping it is applied as the last stateful inspection step.

Flow-based inspection

Flow-based inspection identifies and blocks security threats in real time as they are identified.

Flow-based inspection samples packets in a session and uses single-pass Direct Filter Approach (DFA) pattern matching to identify possible attacks or threats. Depending on the options selected in the firewall policy that

accepted the session, flow-based inspection can apply **IPS**, **Application Control**, **Web Filtering**, **DLP** and **Antivirus**.

All of the applicable flow-based security modules are applied simultaneously in one pass. IPS, Application Control, Web Filtering and DLP filtering happen together. Flow-based antivirus caches files during protocol decoding and submits cached files for virus scanning while the other matching is carried out.

Flow inspection typically requires less processing resources than proxy inspection and since its not a proxy, flow-based inspection does not change packets (unless a threat is found and packets are blocked). Flow-based inspection cannot apply as many features as proxy inspection (for example, flow-based inspection does not support client comforting and some aspects of replacement messages).

IPS and Application Control are only applied using flow-based inspection. Web Filtering, DLP and Antivirus can also be applied using proxy-based inspection.

Proxy-based inspection

Proxy-based inspection uses a proxy to inspect content traffic (VoIP, HTTP, HTTPS, FTP, email, and others) for threats. The proxy extracts and caches content, such as files and web pages, from a content session and inspects the cached content for threats. Content inspection happens in the following order: **VoIP inspection**, **DLP**, **Email Filtering**, **Web Filtering**, **Antivirus**, and **ICAP**. If no threat is found the proxy relays the content to its destination. If a threat is found the proxy can block the content and replace it with a replacement message.

The proxy can also block VoIP traffic that contains threats. VoIP inspection can also look inside VoIP packets and extract port and address information and open pinholes in the firewall to allow VoIP traffic through.

ICAP intercepts HTTP and HTTPS traffic and forwards it to an ICAP server. The FortiGate unit is the surrogate, or “middle-man”, and carries the ICAP responses from the ICAP server to the ICAP client; the ICAP client then responds back, and the FortiGate unit determines the action that should be taken with these ICAP responses and requests.

Egress packet flow

After stateful inspection and flow or proxy-based inspection the packet goes through the following steps before exiting.

IPsec VPN

If the packet is to be sent out an IPsec tunnel, it is at this stage the encryption and required encapsulation is performed.

Source NAT (SNAT)

The FortiGate unit checks the NAT table and determines if the source IP address for outgoing traffic must be changed using SNAT. SNAT is typically applied to traffic from an internal netwotk heading out to the Internet. SNAT means the actual address of the internal network is hidden from the Internet.

DNAT must take place before routing so that the FortiGate unit can route the packet to the correct destination.

Routing

The final routing step determines the next hop router to send the packet to after it exits the FortiGate unit.

Interface TCP/IP Stack

Egress packets are received by the interface network device driver which forwards the packet out the interface an onto the network.

Comparison of inspection types

The tables in this section show how different security functions map to different inspection types.

Mapping security functions to inspection types

The table below lists FortiOS security functions and shows whether they are applied during stateful inspection, flow-based inspection or proxy-based inspection.

FortiOS security functions and inspection types

Security Function	Stateful Inspection	Flow-based inspection	Proxy-based inspection
Firewall	yes		
IPsec VPN	yes		
Traffic Shaping	yes		
User Authentication	yes		
Management Traffic	yes		
SSL VPN	yes		
IPS		yes	
Antivirus		yes	yes
Application Control		yes	
Web filtering		yes	yes
DLP		yes	yes
Email Filtering			yes
VoIP inspection			yes
ICAP			yes

More informaion about inspection methods

The three inspection methods each have their own strengths and weaknesses. The following table looks at all three methods side-by-side.

Inspection methods comparison

Feature	Stateful	Flow	Proxy
Inspection unit per session	first packet	selected packets	complete content
Memory, CPU required	low	medium	high
Level of threat protection	good	better	best
Authentication	yes		
IPsec and SSL VPN	yes		
Antivirus protection		yes	yes
Web Filtering		yes	yes
Data Leak Protection (DLP)		yes	yes
Application control		yes	
IPS		yes	
Delay in traffic	minor	no	small
Reconstruct entire content		no	yes

Client/Server connection packet flow example

The following example illustrates the flow of a packet that is part of a session between a client and a web server with authentication, FortiGuard Web Filtering and antivirus.

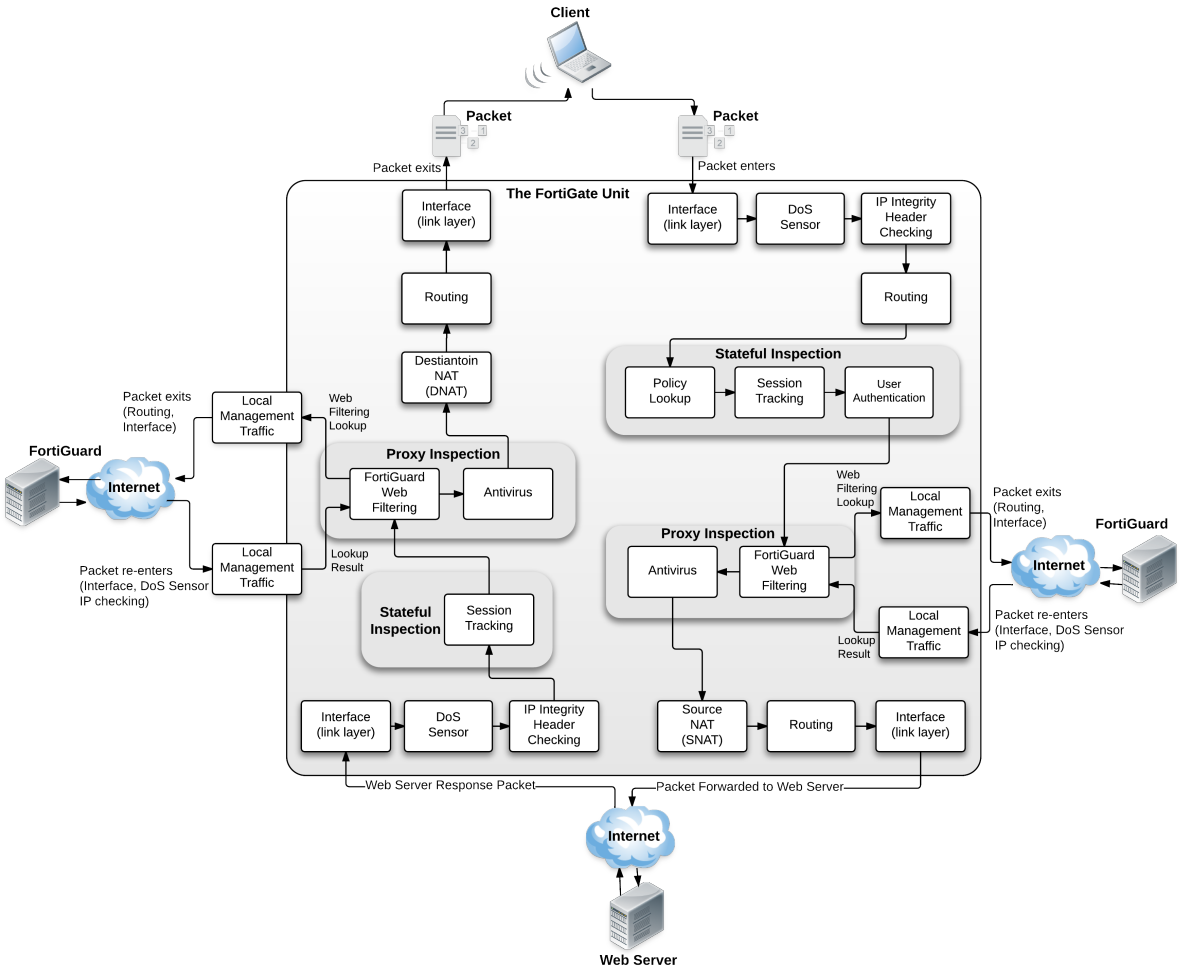
Initiating connection from client to web server

1. Client sends packet to web server.
2. The packed is routed to a FortiGate interface.
3. DoS sensor checks to ensure the sender is valid and not attempting a denial of service attack.
4. IP integrity header checking. If the packet is OK it continues, otherwise it is dropped.
5. Routing.
6. Policy lookup.
7. User authentication.
8. Proxy-based inspection:
   - FortiGuard Web Filtering (FortiGuard web filtering lookup)
   - Antivirus
9. Source NAT changes the source address to the FortiGate IP address
10. Routing
11. Interface transmission to network
12. Packet forwarded to web server

Response from web server

1. Web Server sends response packet to client.
2. The packed is routed to a FortiGate interface
3. DoS sensor checks to ensure the sender is valid and not attempting a denial of service attack.
4. IP integrity header checking. If the packet is OK it continues, otherwise it is dropped.
5. Stateful inspection recognizes the packet is part and an established session.
6. Source NAT changes the destination address from the FortiGate interface to the client IP address
7. Proxy-based inspection:
   - FortiGuard Web Filtering (FortiGuard Web Filtering lookup)
   - Antivirus
6. Destination NAT changes the destination address to the client IP address
7. Packet is routed to the client.
8. Interface transmission to network
9. Packet returns to client

Life of a packet - Client/server connection



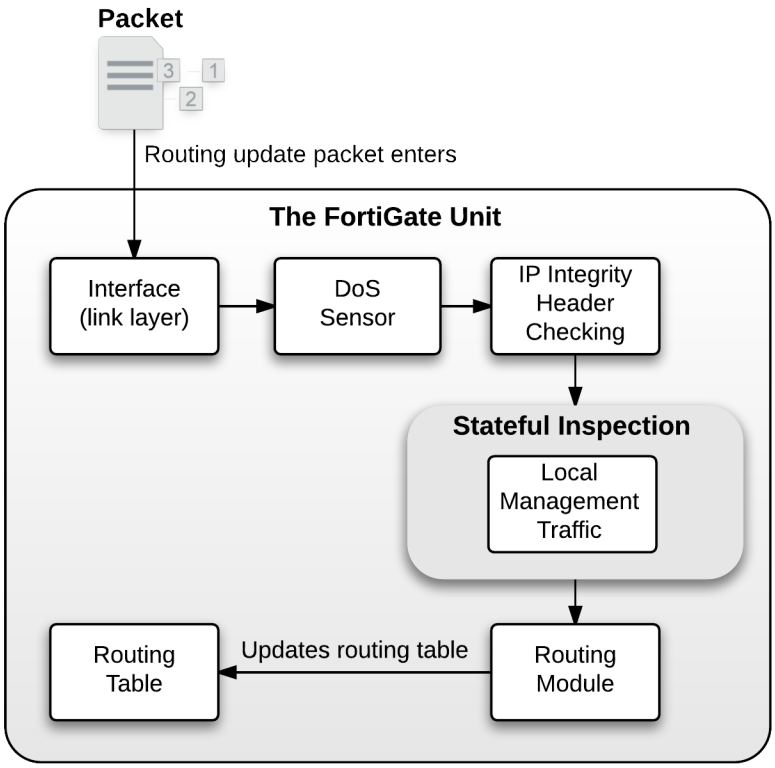
Routing table update packet flow example

The following example illustrates the flow of a packet when there is a routing table update. As this is low level, there is no security involved. This example includes the following steps:

1. FortiGate unit receives routing update packet
2. Packet intercepted by FortiGate unit interface.
3. DoS sensor checks to ensure the sender is valid and not attempting a denial of service attack.
4. IP integrity header checking. If the packet is OK it continues, otherwise it is dropped.
5. Stateful policy engine
   Local Management traffic
6. Routing module
   Update routing table

The figure below illustrates the process steps.

Life of a Packet - Routing table update



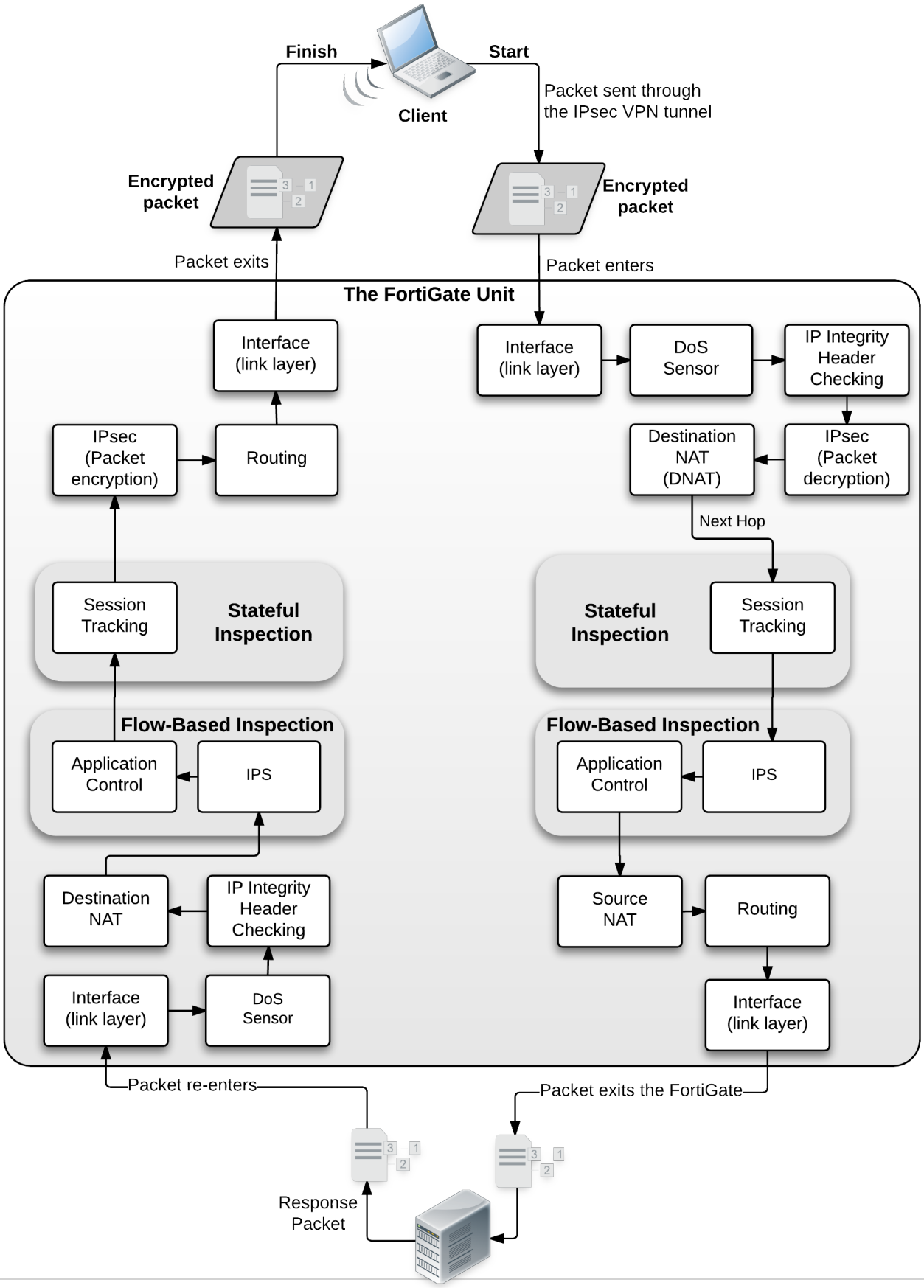
Dialup IPsec VPN with Application control example

This example includes these steps:

1. FortiGate unit receives IPsec encrypted packet from Internet
2. Packet intercepted by FortiGate unit interface.
3. DoS sensor checks to ensure the sender is valid and not attempting a denial of service attack.
4. IP integrity header checking. If the packet is OK it continues, otherwise it is dropped.
5. IPsec
   - Packet matches IPsec phase 1
   - Packet is unencrypted
6. Destination NAT
7. Next hop route
8. Stateful Inspection
   - Session Tracking
9. Flow-based inspection
   - IPS
   - Application Control
10. Source NAT
11. Routing
12. Interface transmission to network
13. Packet forwarded to internal server

Response from server

1. Server sends response packet
2. Packet intercepted by FortiGate unit interface
3. DoS sensor checks to ensure the sender is valid and not attempting a denial of service attack.
4. IP integrity header checking. If the packet is OK it continues, otherwise it is dropped.
5. Destination NAT
6. Flow-based inspection
   - IPS
   - Application Control
7. Stateful Inspection
   - Session Tracking
8. IPsec
   - Packet is encrypted
9. Routing
10. Interface transmission to network
11. Encrypted Packet returns to internet


Finish
Start
Client
Packet sent through the IPsec VPN tunnel
Encrypted packet
Encrypted packet
Packet exits
Packet enters
The FortiGate Unit
Interface (link layer)
Interface (link layer)
DoS Sensor
IP Integrity Header Checking
IPsec (Packet encryption)
Routing
Destination NAT (DNAT)
IPsec (Packet decryption)
Next Hop
Session Tracking
Stateful Inspection
Stateful Inspection
Session Tracking
Flow-Based Inspection
Application Control
IPS
Flow-Based Inspection
Application Control
IPS
Destination NAT
IP Integrity Header Checking
Source NAT
Routing
Interface (link layer)
DoS Sensor
Interface (link layer)
Packet re-enters
Packet exits the FortiGate
Response Packet
Internal Server